solidwall

Why is it necessary to protect web applications?

Web technologies are becoming more widespread. They are used everywhere to create a wide variety of applications and services - from promo sites to distributed e-commerce systems, enterprise management systems, and governmental information services.

However, web technologies imply **significant risks**. According statistics, attacks on web applications are among the most common causes of IT security incidents, and the damage can be tremendous. Therefore, web application security must be a high priority for any organization.

Intelligent Web Application Firewall **SolidWall WAF** is the solution that allows to effectively protect (secure) the customer's critical web resources from external attacks.

Secondly, it is possible provide effective protection of the customer's critical web resources against external attacks, and full control of usage applications in allowed scripts.

Key Benefits

High level of protection

High degree of protection from both widespread simple and advanced types of attack through building the most detailed application model along with pattern-matching and semantic methods of abnormal traffic detection.

Effective protection against false positives

False positives early suppression mechanism makes it possible to minimize affection on decision-making enabling WAF operator and focus on real events.

Unique functions of business logic analysis

Users definition and their actions in application, action parameters and data. Such information is used for false positives early suppression, positive model construction of application or it can be passed to other systems for further analysis.

Special machine learning algorithms

Provide ability to optimize WAF performance, detect false positives, automatically build model of applications, use effectively WAF in Security Development Life Cycle (SDLC).

Monitoring	Reports	Integration with 3rd party Systems

Response and Decision Making

False positives suppression

| Requests classification	Pattern matching	Detection of deviation from positive model	Detection of Brute Force attacks
Protocol validation	Complete data parsing	Business logic identification	Identification and authorization control
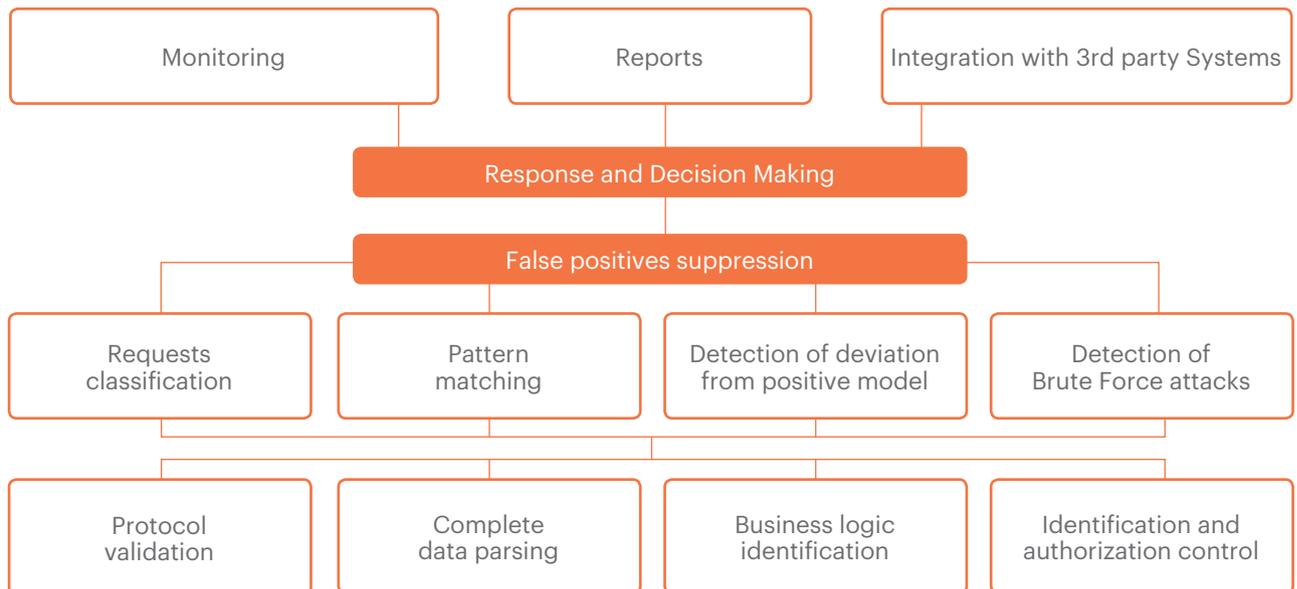
Solution architecture

In deploying at customers site, system architecture provides various ways of installation as well as scalability and reliability.

Database and system management

- Centralized management of multiple analyzers
- Support for unlimited number of applications
- Data replication
- Integration with third party systems via Syslog, SQL, SNMP, REST API
- Blueprints for integration with MicroFocus ArcSight, IBM Qradar, Splunk, Zabbix

Analyzer

- Operation modes: Blocking, Mirroring, PCAP processing of Web server logs and dumps
- Support for High availability: Active-Active, Active-Passive
- SSL termination and Load balancing
- Software bypass mode provides high availability of services even in the event of WAF modules failure or excessive load

Management System
DataBase
[hot standby, replication]

Analyser

Web application servers

User

Internet

Analyzer
[hot standby]
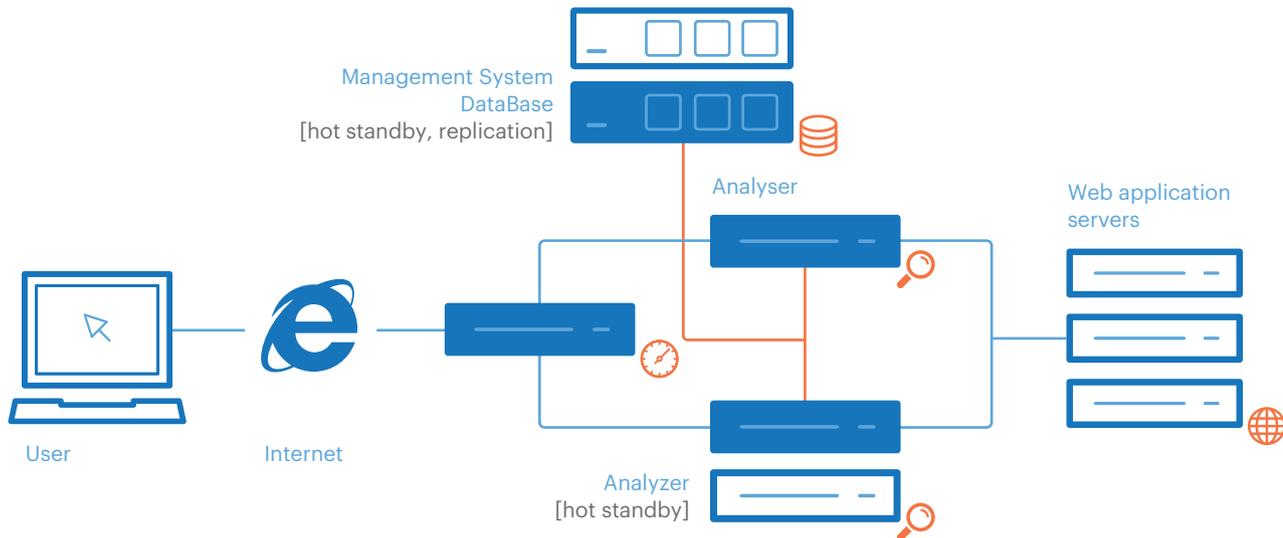
Management interface

Modern graphical management interface improves process of monitoring and configuration, reduces resources and requirements for competency of the WAF operator.

The main features of web interface are:

- Centralized management of all installation nodes in one interface
- Graphical representation of the protected application models
- Convenient monitoring system with a set of panels and information security events grouping. Ability to limit the amount of incoming information
- Configuration settings versioning
- Role-based access to interface functions and detailed audit of user actions
- Multitenancy mode support (for service providers)
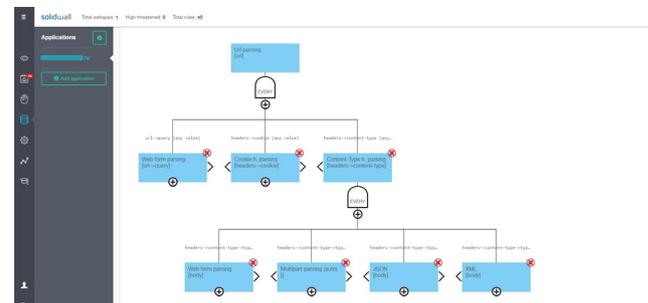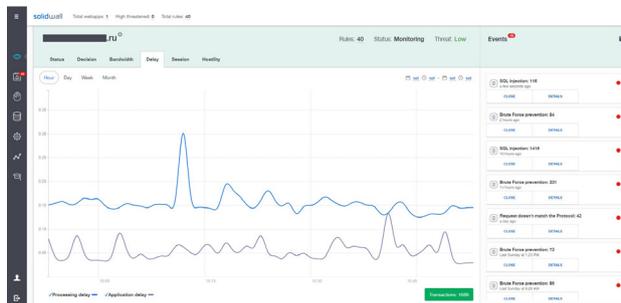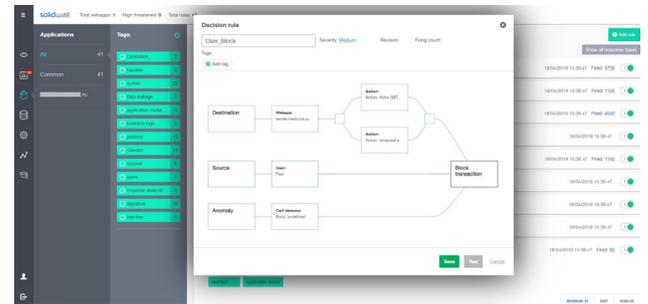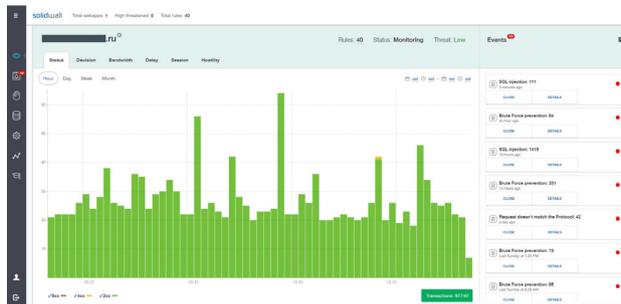
Professional Services

Professional services from the vendor on implementation and the system configuration, monitoring and incidents response provide maximum efficiency of the system usage.

Services include:

- Web application security analysis and POC testing of the proposed solution to assess its potential effectiveness
- Technical design, implementation and fine-tuning of SolidWall WAF, integration with third-party systems
- Change in WAF functionality on client request
- Provide technical training on how-to-work with the system and fundamentals on how to prevent threats in modern Web
- Provide technical and consulting support from experts in the SDLC field and web application protection
- Monitoring of information security incidents, taking action according the prescribed SLA, assistance in incidents investigation
- Preparation of consolidated periodic reports on monitoring/analysis results

Delivery options and licensing scheme

The solution can be delivered in various ways for implementation on the customer's platform:

[Software application]
[Virtual appliance]
[Hardware appliance]

StormWall™ NGENIX

The solution can be acquired as a cloud service together with the AntiDDoS solution by **StormWall** or as a part of the CDN platform by **NGENIX.**

Comparison of system editions	SolidWall WAF Core	SolidWall WAF Basic	SolidWall WAF Pro	SolidWall WAF Enterprise
Protection against OWASP TOP10 web application attacks	●	●	●	●
Effective prevention of false positives, automatic anomalies suppression with high level of false positives	●	●	●	●
Support for prebuild data parsing models of common frameworks and CMS	●	●	●	●
Ability to create and customize data parsing models for in-house applications		●	●	●
Business logic analysis and user session control		●	●	●
Automatic creation of business actions and action parameters for complex applications with active development cycle				●
Support for integration with third party systems (Syslog, SQL, SNMP, REST API), blueprints integration with HPE ArcSight, IBM Qradar, Splunk		●	●	●
Support for distributed, scalable configurations with dedicated analysis nodes and management nodes			●	●
Ability to integrate with SDLC (dedicated interface, license for test zone is free)				●

About SolidSoft

The vendor of the solution, **SolidSoft** is a subsidiary of security laboratory **SolidLab**, which expertize in security analysis services, fine-tuning security systems and implementing secure application development processes (Secure SDLC). The company was established in 2014 and it's a member of **Skolkovo Foundation**.

CONTACTS

LLC SolidSoft

42 Bolshoy boulevard,
Skolkovo Innovation center,
Moscow, Russian Federation, 121205

T. +7 (499) 705-76-57

Official site: www.solidwall.ru
E-mail: info@solidwall.ru